UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/896,438	06/28/2001	Michael Bennett	017887005210	8245

20350 7590 08/11/2005

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
BORLINGHAUS, JASON M	
ART UNIT	**PAPER NUMBER**
3628	

DATE MAILED: 08/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/896,438	BENNETT ET AL.	
	Examiner	Art Unit	
	Jason M. Borlinghaus	3628	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. .See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1 – 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Disclosed Prior Art (applicant's specification) in view of Haverstock (US Patent 6,434,607) and Chapman (D. Brent Chapman & Elizabeth D. Zwicky. Building Internet Firewalls. O'Reilly & Associates Inc. 1995. pp. 45 – 47).

Disclosed Prior Art discloses an information portal system, wherein a user maintains an account at an institution and the institution maintains user data relating to the user at the institution and wherein the user connects to the portal system to have access to user data from one or more institutions ("One portal solution is the "stand-in" system, where a portal operator stands in place of the user to get data from the financial institution. Fig. 1 is a block diagram of such a system. As shown there, a user interacts

with the system using a user client 12 that is coupled to a portal site 14. Portal site 14 is shown comprising a portal server 16 and a stored user authentication database 18. Portal server 16 is coupled to a financial institution (F1) server 20 at a financial institution, which is shown coupled to a user account database 22." – see specification, page 2), the information portal system comprising:

- a portal server including logic to authenticate a user logging onto the portal server for a portal session from a user client. ("To set up a stand-in arrangement, the user sets up an account with a portal operator, including portal user authentication data, such as a user ID and password that authenticates the user to the portal." – see specification, page 2);
- an institution server (financial institution server) including logic to authenticate a user to provide the user with access to the user's data at the institution and to allow the user to perform an action (information retrieval/transaction) relating to the user's data ("The user then provides the portal operator with all the financial institution authentication data the user uses to connect to the financial institution servers and an indication of the financial institution (e.g., domain name, URL, or IP address). The portal operator stores the user's financial institution authentication data at its servers. When the user makes a request for information from the portal, the portal server connects to the financial institution server and, using the user authentication data, logs on as the user and gets the information it needs." – see specification, page 2. "Consequently, there is a risk that if a

database of user IDs and passwords stored at the portal is compromised, the attacker could then access many users' financial institution accounts and even make transactions on those accounts." – see specification, page 3 – establishing that transactions can be performed on the institution servers provided proper authentication was achieved.)

- a portal-institution interface over which the portal system authenticates the portal system to the institution server. ("When the user makes a request for information from the portal, the portal server connects to the financial institution server and, using the user authentication data, logs on as the user and gets the information it needs." – see specification, page 2);
- logic at the portal server to perform on the user's data an action (information retrieval) using requests to the institution server after authenticating the portal server to the institution server. ("When the user makes a request for information from the portal, the portal server connects to the financial institution server and, using the user authentication data, logs on as the user and gets the information it needs." – see specification, page 2); and
- wherein the institution is a financial institution. (supra – see specification, page 2); and
- wherein the user data is financial transaction information ("When the user makes a request for information from the portal, the portal server connects to the financial institution server and, using the user authentication data,

logs on as the user and gets the information it needs." – see specification, page 2 – establishing the obtainment of financial transaction information from the financial institution server).

Disclosed Prior Art does not teach an information portal system comprising:

- an institution server including logic to authenticate a user to provide the user with access to the user's data at the institution and to allow the user to perform an action selected from a first set of actions relating to the user's data;
- logic at the portal server to perform on the user's data an action selected from the first set of actions using requests to the institution server after authenticating the portal server to the institution server;
- wherein the actions performable on the user's data by the portal are actions selected from a second set of actions that is a proper subset of the first set of actions;
- the first set of actions includes conducting a financial transaction and the second set of actions includes viewing user data but the second set of actions does not include conducting financial transactions.

Providing different users of a system with different levels of access and allowing them different subsets of actions on the system, such as through a least privilege designation or through role-based security, is old and well known in the art of computer and network security. As evidenced by Haverstock, disclosing a web-based server utilizing a role-based security system, in which Haverstock states, "The system also

provides role-based, multi-level security module 40 for controlling access to objects within the system. The system enables an authorized individual to assign users a defined role. Each role may have various privileges based on the priority level of the role. Priority levels may comprise a read only privilege, read and edit privileges, read public information only privileges, etc." (see col. 5, lines 56 – 62).

Furthermore, Chapman, disclosing the use of least privilege designations for network security purposes, states, "Basically, the principle of least privilege means that any object (user, administrator, program, system, whatever) should have only the privileges the object needs to perform its assigned tasks – and no more...In the Internet context, the examples are endless. Every user probably doesn't need to access every Internet service. Every user probably doesn't need to modify (or even read) every file on your system...Applying the principle of least privilege suggests that you should explore ways to reduce the privileges required for various operations." (see page 45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Disclosed Prior Art by incorporating commonly known security measures, such as the least privilege principle, role-based security or access control lists, as were disclosed by Haverstock and Chapman, to limit the portal server's actions on the institution server to a subset of the total actions that the user, him/herself, could employ on the institution server, as the portal server would be deemed a non-trusted third party and not the user, him/herself.

In particular, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Disclosed Prior Art, Haverstock and

Chapman to have limited the portal server, in the role of non-trusted third party, to access and retrieve user information, the least privilege required as an information portal, and not allowing the portal server to act or authorize transactions based upon that user information, as such activities would be outside its scope as an information portal.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jason M. Borlinghaus whose telephone number is (571) 272-6924. The examiner can normally be reached on 8:30am-5:00pm M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hyung Sough can be reached on (571) 272-6799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

***

HYUNG SOUGH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600